The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
11/18/2020

SUBJECT:
Multiple Vulnerabilities in Google Chrome Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Google Chrome, the most severe of which could allow for arbitrary code execution. Google Chrome is a web browser used to access the Internet. Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute arbitrary code in the context of the browser. Depending on the privileges associated with the application, an attacker could view, change, or delete data. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- Google Chrome versions prior to 87.0.4280.66

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Google Chrome, the most severe of which could allow for arbitrary code execution. These vulnerabilities can be exploited if a user visits, or is redirected to, a specially crafted web page. Details of the vulnerabilities are as follows:

- A security vulnerability due to use after free error. Specifically, this issue affects the 'payments' component. (CVE-2020-16018)

- A security vulnerability due to an improper implementation in 'filesystem'. (CVE-2020-16019)
- A security vulnerability due to an improper implementation in 'cryptohome'. (CVE-2020-16020)
- A security vulnerability due to a race condition in 'ImageBurner' component. (CVE-2020-16021)
- A security vulnerability because it fails to properly enforce policy in 'networking'. (CVE-2020-16022)
- A security vulnerability that occurs because it fails to properly validate data in 'WASM'. (CVE-2020-16015)
- A security vulnerability due to use after free error. Specifically, this issue affects the 'PPAPI' component. (CVE-2020-16014)
- A security vulnerability due to use after free error. Specifically, this issue affects the 'WebCodecs' component. (CVE-2020-16023)
- A heap-based buffer-overflow vulnerability. Specifically, this issue affects the 'UI' component. (CVE-2020-16024)
- A heap-based buffer-overflow vulnerability. Specifically, this issue affects the 'clipboard' component. (CVE-2020-16025)
- A security vulnerability due to use after free error. Specifically, this issue affects the 'WebRTC'. (CVE-2020-16026)
- A security vulnerability because it fails to properly enforce policy in 'developer tools'. (CVE-2020-16027)
- A heap-based buffer-overflow vulnerability. Specifically, this issue affects the 'WebRTC'. (CVE-2020-16028)
- A security vulnerability due to an improper implementation in 'PDFium' library. (CVE-2020-16029)
- A security vulnerability that occurs because it fails to properly validate data in 'Blink'. (CVE-2020-16030)
- A security vulnerability due to improper security UI in 'tab preview'. (CVE-2020-16031)
- A security vulnerability due to improper security UI in 'sharing'. (CVE-2020-16032)
- A security vulnerability due to improper security UI in 'WebUSB'. (CVE-2020-16033)
- A security vulnerability due to an improper implementation in 'WebRTC'. (CVE-2020-16034)
- A security vulnerability that occurs because it fails to properly validate data in 'cros-disks'. (CVE-2020-16035)
- A security vulnerability due to an improper implementation in 'cookies'. (CVE-2020-16036)

Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute arbitrary code in the context of the browser. Depending on the privileges associated with the application, an attacker could view, change, or delete data. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

RECOMMENDATIONS:
The following actions should be taken:
- Apply the stable channel update provided by Google to vulnerable systems immediately after appropriate testing.

- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

Google:

https://chromereleases.googleblog.com/2020/11/stable-channel-update-for-desktop_17.html

CVE:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16018
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16019
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16020
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16021
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16022
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16015
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16014
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16023
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16024
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16025
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16026
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16027
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16028
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16029
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16030
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16031
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16032
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16033
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16034
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16035
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16036